EXHIBIT 1

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means ❒ Original ❒ Duplicate Original

UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* APPLE iPHONE SE, MODEL A1662, IMEI NUMBER 353792084620967, CURRENTLY LOCATED AT THE FEDERAL BUREAU OF INVESTIGATION IN QUANTICO, VIRGINIA	)	Case No.1:22-SW-462

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Eastern District of Virginia *(identify the person or describe the property to be searched and give its location)*:

DESCRIPTION, as described in Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before September 8, 2022 *(not to exceed 14 days)*

☑ in the daytime 6:00 a.m. to 10:00 p.m. ❒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Hon. John F. Anderson .

(United States Magistrate Judge)

❒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

❒ for _____ days *(not to exceed 30)* ❒ until, the facts justifying, the later specific date of _____ .

Date and time issued: 08/26/2022 11:45 am

John F. Anderson Digitally signed by John F. Anderson Date: 2022.08.26 11:56:20 -04'00'

Judge's signature

City and state: Alexandria, Virginia

The Honorable John F. Anderson, U.S. Magistrate Judge

Printed name and title

Return

Case No.: 1:22-SW-462	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

The property to be searched is an Apple iPhone SE, Model A1662, with International Mobile Equipment Identity number 353792084620967 and further identified by the FBI as a Portable Electronic Device, evidence number 1B290, hereinafter the "Device." The Device is currently in the custody of the FBI's Electronic Device Analysis Unit in Quantico, Virginia.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

I. Items To Be Seized

1. The items to be seized are evidence, contraband, fruits, and/or instrumentalities of violations of 18 U.S.C. § 1115 (Seaman's Manslaughter) (the "Subject Offense"), namely:

a. Evidence relating to the origin of the fire aboard the P/V *Conception* on or about September 2, 2019;

b. Evidence relating to the causation of the fire aboard the P/V *Conception* on or about September 2, 2019;

c. Evidence of custom, defective, and/or non-compliant electrical equipment, systems, and/or components on the P/V *Conception*;

d. Evidence of custom, defective, or non-compliant fire detection or suppression systems on the P/V *Conception*;

e. Evidence of custom, defective, and/or non-compliant passenger safety and/or evacuation structures, systems, and/or procedures on the P/V *Conception*;

f. Data, records, documents (including text messages and/or e-mails), or other materials relating to the Device user's or users' trip aboard the P/V *Conception*;

g. Audio recordings, pictures, video recordings, or still captured images relating to the P/V *Conception*;

h. Any device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offense, and forensic copies thereof.

2. With respect to any Device containing evidence falling within the scope of the foregoing categories of items to be seized:

a. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted;

b. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the attachment of other devices;

d. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

e. evidence of the times the device was used;

f. applications, programs, software, documentation, manuals, passwords, keys, and other access devices that may be necessary to access the device or data stored on the device, to run software contained on the device, or to conduct a forensic examination of the device;

g. records of or information about Internet Protocol addresses used by the device.

3. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

II. Search Procedure for Digital Devices

4. In searching the Device (or forensic copies thereof), law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") may search any device capable of being used to facilitate the Subject Offense or containing data falling within the scope of the items to be seized.

b. The search team will, in its discretion, either search the Device where it is currently located or transport it to an appropriate law enforcement laboratory or similar facility to be searched at that location.

c. The search team shall complete the search of the Device as soon as is practicable but not to exceed 120 days from the date of issuance of the warrant. The government will not search the digital device and/or forensic images thereof beyond this 120-day period without obtaining an extension of time order from the Court.

d. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

    i. The search team may subject all of the data contained in any Device capable of containing any of the items to be seized to the search protocols to determine whether the Device and any data thereon falls within the scope of the items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the scope of the items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched..

iii. The search team may use forensic examination and searching tools, such as "EnCase," "Griffeye," and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

e. The search team will not seize contraband or evidence relating to other crimes outside the scope of the items to be seized without first obtaining a further warrant to search for and seize such contraband or evidence.

f. If the search determines that the Device does not contain any data falling within the list of items to be seized, the government will, if and as soon as is practicable, return the Device and delete or destroy all forensic copies thereof.

g. If the search determines that the Device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

h. If the search determines that the Device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

i. The government may also retain the Device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in

circumstances where the government has not been able to fully search the device because the device or files contained therein is/are encrypted.

j. After the completion of the search of the Device, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

5. The review of the electronic data obtained pursuant to this warrant may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

6. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

AO 106A (08/18) Application for a Warrant by Telephone or Other Reliable Electronic Means

UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
APPLE iPHONE SE, MODEL A1662, IMEI NUMBER 353792084620967, CURRENTLY LOCATED AT THE FEDERAL BUREAU OF INVESTIGATION IN QUANTICO, VIRGINIA

Case No. 1:22-SW-462

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

DESCRIPTION, as described in Attachment A.

located in the Eastern District of Virginia, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 1115	Misconduct or neglect of ship officers

The application is based on these facts:

☑ Continued on the attached sheet.

☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Kurt Sorensen
SAUSA (NAME)/AUSA (NAME)

Special Agent Joseph Hamer, FBI
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: 8/26/2022

John F. Anderson Digitally signed by John F. Anderson Date: 2022.08.26 11:55:57 -04'00'
Judge's signature

City and state: Alexandria, Virginia

Hon. John F. Anderson, U.S. Magistrate Judge
Printed name and title

ATTACHMENT A

The property to be searched is an Apple iPhone SE, Model A1662, with International Mobile Equipment Identity number 353792084620967 and further identified by the FBI as a Portable Electronic Device, evidence number 1B290, hereinafter the "Device." The Device is currently in the custody of the FBI's Electronic Device Analysis Unit in Quantico, Virginia.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

I. Items To Be Seized

1. The items to be seized are evidence, contraband, fruits, and/or instrumentalities of violations of 18 U.S.C. § 1115 (Seaman's Manslaughter) (the "Subject Offense"), namely:

a. Evidence relating to the origin of the fire aboard the P/V *Conception* on or about September 2, 2019;

b. Evidence relating to the causation of the fire aboard the P/V *Conception* on or about September 2, 2019;

c. Evidence of custom, defective, and/or non-compliant electrical equipment, systems, and/or components on the P/V *Conception*;

d. Evidence of custom, defective, or non-compliant fire detection or suppression systems on the P/V *Conception*;

e. Evidence of custom, defective, and/or non-compliant passenger safety and/or evacuation structures, systems, and/or procedures on the P/V *Conception*;

f. Data, records, documents (including text messages and/or e-mails), or other materials relating to the Device user's or users' trip aboard the P/V *Conception*;

g. Audio recordings, pictures, video recordings, or still captured images relating to the P/V *Conception*;

h. Any device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offense, and forensic copies thereof.

2. With respect to any Device containing evidence falling within the scope of the foregoing categories of items to be seized:

a. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted;

b. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the attachment of other devices;

d. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

e. evidence of the times the device was used;

f. applications, programs, software, documentation, manuals, passwords, keys, and other access devices that may be necessary to access the device or data stored on the device, to run software contained on the device, or to conduct a forensic examination of the device;

g. records of or information about Internet Protocol addresses used by the device.

3. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

II. Search Procedure for Digital Devices

4. In searching the Device (or forensic copies thereof), law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") may search any device capable of being used to facilitate the Subject Offense or containing data falling within the scope of the items to be seized.

b. The search team will, in its discretion, either search the Device where it is currently located or transport it to an appropriate law enforcement laboratory or similar facility to be searched at that location.

c. The search team shall complete the search of the Device as soon as is practicable but not to exceed 120 days from the date of issuance of the warrant. The government will not search the digital device and/or forensic images thereof beyond this 120-day period without obtaining an extension of time order from the Court.

d. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

    i. The search team may subject all of the data contained in any Device capable of containing any of the items to be seized to the search protocols to determine whether the Device and any data thereon falls within the scope of the items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the scope of the items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched..

iii. The search team may use forensic examination and searching tools, such as "EnCase," "Griffeye," and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

e. The search team will not seize contraband or evidence relating to other crimes outside the scope of the items to be seized without first obtaining a further warrant to search for and seize such contraband or evidence.

f. If the search determines that the Device does not contain any data falling within the list of items to be seized, the government will, if and as soon as is practicable, return the Device and delete or destroy all forensic copies thereof.

g. If the search determines that the Device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

h. If the search determines that the Device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

i. The government may also retain the Device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in

circumstances where the government has not been able to fully search the device because the device or files contained therein is/are encrypted.

j. After the completion of the search of the Device, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

5. The review of the electronic data obtained pursuant to this warrant may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

6. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

IN THE MATTER OF THE SEARCH OF AN APPLE iPHONE SE, MODEL A1662, IMEI NUMBER 353792084620967, CURRENTLY LOCATED AT THE FEDERAL BUREAU OF INVESTIGATION IN QUANTICO, VIRGINIA	Case No. 1: 22-SW-462

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, JOSEPH HAMER, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been so employed since May 1, 2016. As a federal agent, I am empowered by United States law to conduct investigations regarding, and make arrests for, offenses enumerated in Title 18 of the United States Code. Since April 1, 2019, I have been assigned to work violent crimes against children at the FBI's Ventura Resident Agency in Ventura County, California. Prior to my assignment at the FBI's Ventura Resident Agency, I was assigned to the Los Angeles Violent Crime Task Force. During my tenure as a Special Agent, I have conducted and participated in numerous investigations of criminal activity, executed search and arrest warrants, and seized evidence of federal criminal violations. I have received both formal and informal training from

the FBI regarding computer-related investigations and computer technology. My formal law enforcement training includes 21 weeks of education at the FBI Academy, where I took classes on writing affidavits and providing evidentiary testimony, among other topics.

3. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

4. The property to be searched is an Apple iPhone SE, Model A1662, with International Mobile Equipment Identity ("IMEI") number 353792084620967 and further identified by the FBI as a Portable Electronic Device, evidence number 1B290, hereinafter the "Device." The Device is currently in the custody of the FBI's Electronic Device Analysis Unit (the "EDAU") in Quantico, Virginia.

5. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

A. Probable Cause to Search the Device

6. On September 7, 2019, Special Agent Jaime Wray of the United States Coast Guard Investigative Service obtained a federal search warrant in the Central District of California issued by the Honorable Louise A. LaMothe, United States Magistrate Judge, related to the fatal fire onboard the passenger vessel ("P/V") *Conception* near Santa Cruz Island, California on September 2, 2019. (*See* C.D. Cal. Case No. 2:19-MJ-03738.) That warrant, attached hereto as Exhibit 1, authorized the search of the P/V *Conception* wreckage as well as

any digital devices recovered from the wreckage and debris field. The warrant further authorized the seizure of evidence, contraband, fruits, and/or instrumentalities of violations of 18 U.S.C. § 1115 (Seaman's Manslaughter). The application in support of that warrant, attached hereto as Exhibit 2, set forth, among other things, probable cause supporting the issuance of the warrant. Exhibits 1 and 2 are incorporated herein by reference.

7. The Device was recovered from the P/V *Conception* wreckage debris field and seized pursuant to the attached search warrant. The search of the Device thus was authorized pursuant to the attached search warrant. The Device has remained in law enforcement custody, as described further below, since its initial seizure.

B. Request for Second Search Warrant for the Device

8. Following its recovery from the P/V *Conception* wreckage debris field, the Device was initially inventoried in evidence by federal law enforcement in Ventura County, California. The FBI subsequently transferred the Device to the EDAU in Quantico, Virginia to attempt to extract data from the device. As a general matter, this process is technical and time-consuming. The process was made more difficult based on the condition in which the Device was found. Specifically, the Device sustained fire and water damage because it was collected from the Pacific Ocean after the P/V *Conception* sank due to a fire, as described in more detail in the affidavit included in Exhibit 2.

9. Based on information provided to me by the EDAU, I understand that, upon an initial review of the Device, the EDAU determined that traditional methods of extracting data from the device likely would not be feasible due to the damage the Device had sustained. As part of that initial review, the EDAU identified the Device as a potential candidate for an alternative approach involving the removal and analysis of certain components of the Device

using certain forensic tools. This enhanced forensic approach involves a delicate, highly technical, and time-consuming process in a laboratory setting and has no guarantee of success.

10. The EDAU has not yet attempted to undertake this alternative approach with respect to the Device, for which it still maintains custody in Quantico, Virginia. Among other things, due to the ongoing COVID-19 pandemic, and especially during the most difficult periods of the pandemic during 2020 and 2021, the work schedules of the laboratory and personnel responsible for the extraction of data from the Device has been materially impacted. The majority of their work needs to be completed in the laboratory setting, but at various points the laboratory has limited the number of personnel allowed to work at any given time.

11. Due to these and other related limitations during the pandemic, the EDAU also has experienced a substantial backlog of digital devices received from law enforcement, both domestically and internationally, that need to be processed for review. This backlog has further impacted the EDAU's ability to undertake the enhanced forensic review required for the Device.

12. As explained above, the Device is currently in the lawful possession of the FBI upon being recovered from the P/V *Conception* wreckage debris field. The FBI already obtained one prior search warrant (Exhibit 1) to review the contents of the Device for responsive information. However, because that initial search warrant has expired, I am requesting a new search warrant in order to search the Device and seize materials listed in Attachment B here to, to the extent any data can be extracted from the Device.[1]

---

[1] Consistent with the general practice for digital device search warrants in the Central District of California, Attachment B-4 to the initial warrant provided for a 120-day period for the government to complete its search of any devices recovered from the wreckage debris field of the P/V *Conception*, absent a further court order extending the time for the search. (*See* Exh. 1,

13. The Device is currently in storage at the FBI's EDAU facility in Quantico, Virginia. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of the FBI.

TECHNICAL TERMS

14. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing

---

Attachment B-4 at ¶ 11.a.) Attachment B to the instant search warrant application provides for the same 120-day review period.

and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images and videos. Images and videos can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some

GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

15. Based on my training, experience, and research, I know that the Device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

16. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

17. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

18. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose

many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

19. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it can take a substantial period of time to search a digital device for many reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

c. In addition, as described above, the Device sustained fire and water damage as a result of the fire aboard the P/V *Conception* and the subsequent sinking of the vessel, which has posed additional complications in seeking to extract data from the digital device.

20. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

21. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

CONCLUSION

22. I submit that this affidavit and accompanying exhibits supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

JOSEPH HAMER
Special Agent
Federal Bureau of Investigation

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on August 26th, 2022:

John F. Anderson Digitally signed by John F. Anderson
Date: 2022.08.26 11:55:20 -04'00'

Hon. John F. Anderson
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The property to be searched is an Apple iPhone SE, Model A1662, with International Mobile Equipment Identity number 353792084620967 and further identified by the FBI as a Portable Electronic Device, evidence number 1B290, hereinafter the "Device." The Device is currently in the custody of the FBI's Electronic Device Analysis Unit in Quantico, Virginia.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

I. Items To Be Seized

1. The items to be seized are evidence, contraband, fruits, and/or instrumentalities of violations of 18 U.S.C. § 1115 (Seaman's Manslaughter) (the "Subject Offense"), namely:

a. Evidence relating to the origin of the fire aboard the P/V *Conception* on or about September 2, 2019;

b. Evidence relating to the causation of the fire aboard the P/V *Conception* on or about September 2, 2019;

c. Evidence of custom, defective, and/or non-compliant electrical equipment, systems, and/or components on the P/V *Conception*;

d. Evidence of custom, defective, or non-compliant fire detection or suppression systems on the P/V *Conception*;

e. Evidence of custom, defective, and/or non-compliant passenger safety and/or evacuation structures, systems, and/or procedures on the P/V *Conception*;

f. Data, records, documents (including text messages and/or e-mails), or other materials relating to the Device user's or users' trip aboard the P/V *Conception*;

g. Audio recordings, pictures, video recordings, or still captured images relating to the P/V *Conception*;

h. Any device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offense, and forensic copies thereof.

2. With respect to any Device containing evidence falling within the scope of the foregoing categories of items to be seized:

a. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted;

b. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the attachment of other devices;

d. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

e. evidence of the times the device was used;

f. applications, programs, software, documentation, manuals, passwords, keys, and other access devices that may be necessary to access the device or data stored on the device, to run software contained on the device, or to conduct a forensic examination of the device;

g. records of or information about Internet Protocol addresses used by the device.

3. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

II. Search Procedure for Digital Devices

4. In searching the Device (or forensic copies thereof), law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") may search any device capable of being used to facilitate the Subject Offense or containing data falling within the scope of the items to be seized.

b. The search team will, in its discretion, either search the Device where it is currently located or transport it to an appropriate law enforcement laboratory or similar facility to be searched at that location.

c. The search team shall complete the search of the Device as soon as is practicable but not to exceed 120 days from the date of issuance of the warrant. The government will not search the digital device and/or forensic images thereof beyond this 120-day period without obtaining an extension of time order from the Court.

d. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

    i. The search team may subject all of the data contained in any Device capable of containing any of the items to be seized to the search protocols to determine whether the Device and any data thereon falls within the scope of the items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the scope of the items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched..

iii. The search team may use forensic examination and searching tools, such as "EnCase," "Griffeye," and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

e. The search team will not seize contraband or evidence relating to other crimes outside the scope of the items to be seized without first obtaining a further warrant to search for and seize such contraband or evidence.

f. If the search determines that the Device does not contain any data falling within the list of items to be seized, the government will, if and as soon as is practicable, return the Device and delete or destroy all forensic copies thereof.

g. If the search determines that the Device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

h. If the search determines that the Device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

i. The government may also retain the Device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in

circumstances where the government has not been able to fully search the device because the device or files contained therein is/are encrypted.

j. After the completion of the search of the Device, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

5. The review of the electronic data obtained pursuant to this warrant may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

6. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

[Exhibits 1 and 2 to 1B290 iPhone Search Warrant Application Omitted -- See Footnote 3 in Accompanying Opposition Brief]